Defense Intelligence Strategy

2008

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE
2008

2. REPORT TYPE

3. DATES COVERED
00-00-2008 to 00-00-2008

4. TITLE AND SUBTITLE
Defense Intelligence Strategy

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Department of Defense,Washington,DC

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR’S ACRONYM(S)

11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

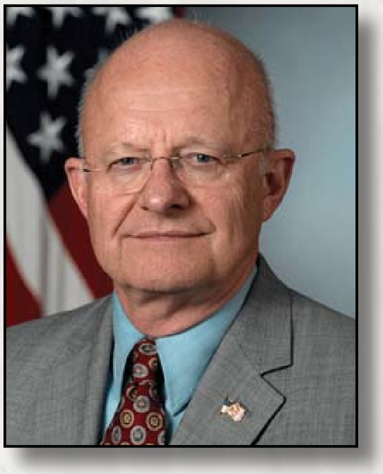
13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**24**	

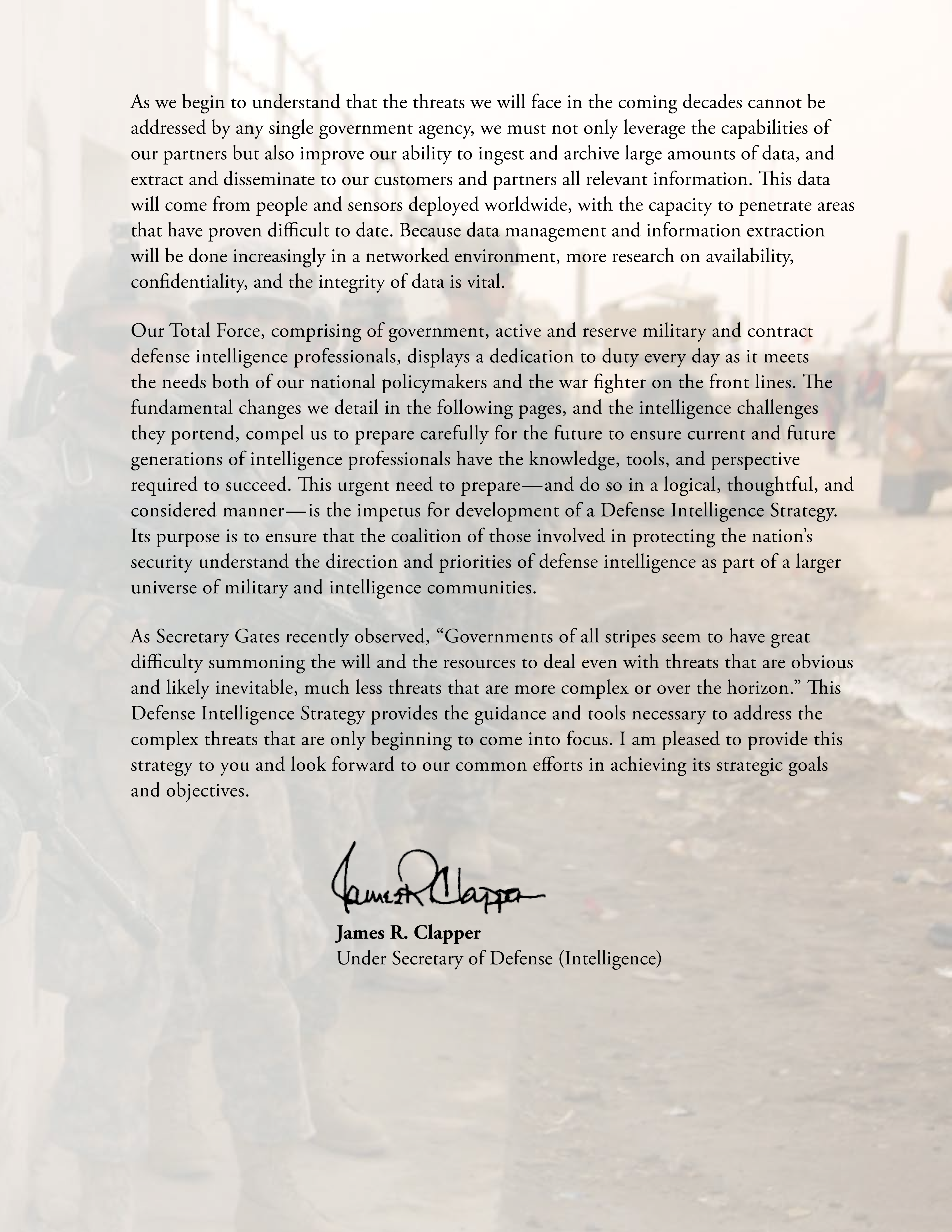
A Message from the Under Secretary of Defense for Intelligence



We are entering an era marked by pace, scope and complexity of change that will challenge the minds and resources of the Defense Intelligence Enterprise. The challenge to provide the information, insight, and warning that allow our national military and civilian leaders to make better decisions both in Washington and on the fields of battle has never been greater or more urgent. It will require a concerted, collective effort by the Department of Defense intelligence, counterintelligence and security communities (Defense Intelligence Enterprise) to protect our military and intelligence assets against all forms and domains of attack and transform the Defense Intelligence Enterprise into one that is agile, global, and diverse.

We have embarked on a fundamental change to the concept of defense intelligence—one that balances the unique role of support to the war fighter with the recognition that today's security environment crosses traditional organizational domains. The deep integration of defense intelligence into the larger Intelligence Community, the evolution of our collaboration with homeland defense counterparts, and the fostering of committed international partnerships are all outcomes of this fundamental change. The Intelligence Community understands that further transformation of the larger national security infrastructure is required to build effectively for the future.

Also undergoing a fundamental change is our concept of "engagement" around the world. As Secretary of Defense Robert Gates noted, "The real challenges we have seen emerge since the end of the Cold War—from Somalia to the Balkans, Iraq, Afghanistan and elsewhere—make clear we in Defense need to change our priorities to be better able to deal with 'asymmetric warfare.' " For defense intelligence professionals, this means our missions will be diverse and multidimensional, punctuated by persistent regional engagements requiring a range of military, humanitarian, and diplomatic capabilities and assets to be used simultaneously. Cultural awareness, social modeling, and language proficiency will be as important as new intelligence systems and technologies. We will need to develop a sizeable cadre of immediately deployable experts with disparate skills. And as the Director of National Intelligence, Michael McConnell, has stated, diversity must be treated as a strategic mission imperative if we are to operate well in this environment.



As we begin to understand that the threats we will face in the coming decades cannot be addressed by any single government agency, we must not only leverage the capabilities of our partners but also improve our ability to ingest and archive large amounts of data, and extract and disseminate to our customers and partners all relevant information. This data will come from people and sensors deployed worldwide, with the capacity to penetrate areas that have proven difficult to date. Because data management and information extraction will be done increasingly in a networked environment, more research on availability, confidentiality, and the integrity of data is vital.

Our Total Force, comprising of government, active and reserve military and contract defense intelligence professionals, displays a dedication to duty every day as it meets the needs both of our national policymakers and the war fighter on the front lines. The fundamental changes we detail in the following pages, and the intelligence challenges they portend, compel us to prepare carefully for the future to ensure current and future generations of intelligence professionals have the knowledge, tools, and perspective required to succeed. This urgent need to prepare—and do so in a logical, thoughtful, and considered manner—is the impetus for development of a Defense Intelligence Strategy. Its purpose is to ensure that the coalition of those involved in protecting the nation's security understand the direction and priorities of defense intelligence as part of a larger universe of military and intelligence communities.

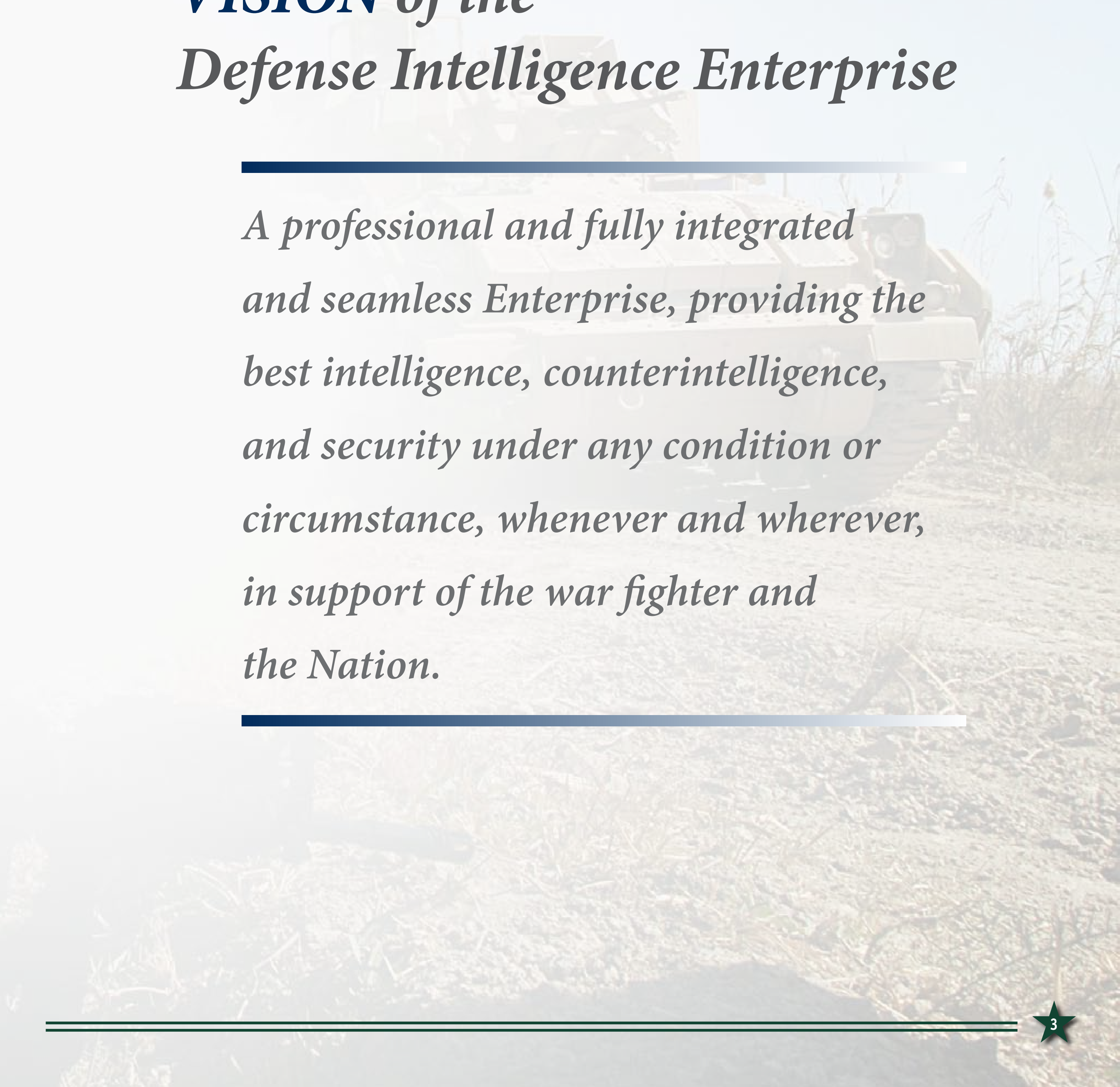
As Secretary Gates recently observed, "Governments of all stripes seem to have great difficulty summoning the will and the resources to deal even with threats that are obvious and likely inevitable, much less threats that are more complex or over the horizon." This Defense Intelligence Strategy provides the guidance and tools necessary to address the complex threats that are only beginning to come into focus. I am pleased to provide this strategy to you and look forward to our common efforts in achieving its strategic goals and objectives.

James R Clapper

James R. Clapper
Under Secretary of Defense (Intelligence)

MISSION of the Defense Intelligence Enterprise

Support our national, defense and international partners with "knowledge rich" all-source defense intelligence, counterintelligence, and security.



VISION of the Defense Intelligence Enterprise

A professional and fully integrated and seamless Enterprise, providing the best intelligence, counterintelligence, and security under any condition or circumstance, whenever and wherever, in support of the war fighter and the Nation.

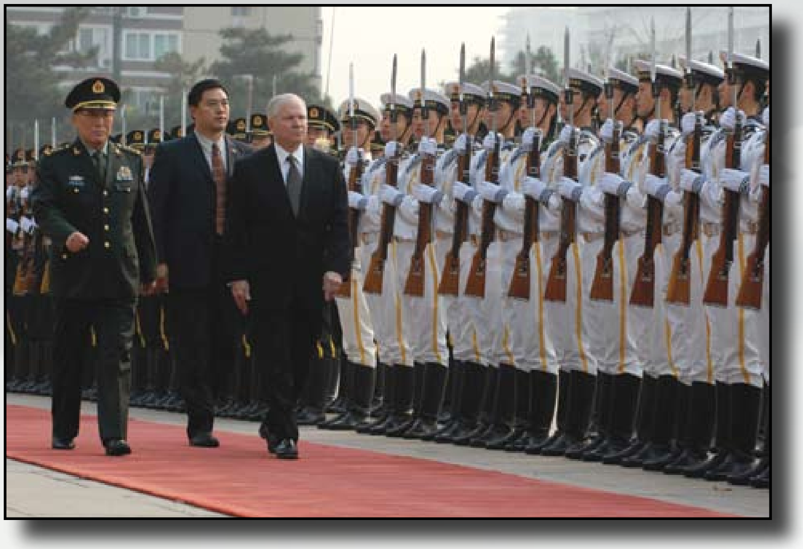
Strategic Environment

21st Century Geopolitical Environment

Defense intelligence today operates in a world markedly different from the one in which it developed. The emergence of a highly interconnected global economy is reshaping international alliances, speeding the adoption of technologies, and giving rise to the development of new economic centers. This interconnected world, while offering opportunities to many, also presents significant national security risks. Regional instability resulting from the spread of religious fundamentalism, massive population shifts, and competition for natural resources and other factors will foster new requirements for defense intelligence. The complex and interrelated forces at work will transform societies and recast the intelligence priorities, strategies, and methods necessary to meet the unique demands of a dynamic 21st century.

- **Transition to Modernity:** The global economy, marked by the growing influence of a middle class supported by the rapid adoption of new technology, will redefine economic and security parameters between the developing and developed worlds. Many societies will embrace the benefits of such progress, although a backlash may occur from those whose expectations are not met or do not have access to resources and technology. This unprecedented acceleration of change and widening of the gap between leaders and laggards may threaten fragile governance institutions. Faced with this highly asymmetric and dynamic framework, intelligence professionals will be called on to consider a security environment marked by regional, economic, resource, and ideological competition.

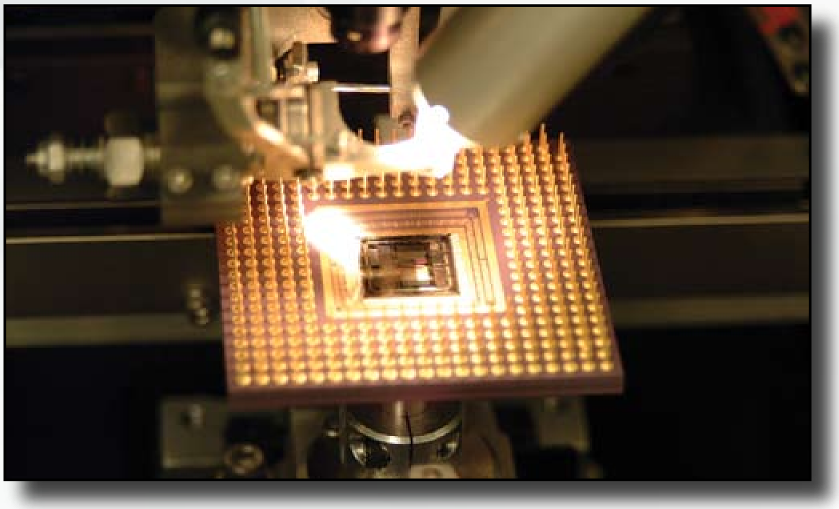
- **Shifting Geopolitical Landscape:** The international community is in a state of considerable flux. The economic and military development of China and the reenergizing of the Russian military are predominant factors among large state actors over the next decades. China's Gross Domestic Product (GDP), growing at an estimated 8% annually, is slated to become second only to the United States' GDP. In Russia, defense spending during 2001 – 2007 has quadrupled and the military has stated plans to replace 45% of the army's hardware by 2015. The strengthening of the European Union's alliance of 27 countries will also give rise to an important new regional strategic identity. These developments, and others around the world, will change the geopolitical landscape intelligence professionals analyze on a daily basis.



- **Urban Population Migration:** By 2020, it is anticipated that two-thirds of the world's population will have migrated to urban environments. High population growth and urban migration will create new demands for housing, infrastructure, health care, education and employment, raising the specter of instability in some regions that could be further exacerbated by a "youth bulge" emerging in the developing world. These patterns, combined with ease of travel and anonymity of communications, could facilitate the spread of terrorism based on violent extremism. This requires defense intelligence professionals to understand cultural dynamics, weapons, operations, finances, recruiting, training and propaganda particularly as terrorist organizations seek the acquisition and use of weapons of mass destruction (WMD).

- **Competition for Natural Resources:** Demand for oil in Asia is expected to double by 2020, with OPEC accounting for production of nearly 50% of the world's oil supply by 2025. Demand for African crude will also rise, significantly changing the economy in some areas. Industrial activity in the developing world will create important global climate and security considerations. In the Artic region, sea ice has receded by 40% since 1979, causing new territorial disputes. Scarcity of clean, non-toxic water will also be a major concern. By 2025, in approximately 54 countries, housing nearly half the world's population, supply will fall short of water demands. These significant resource issues will underlie regional actions and jeopardize stability, creating an important focus of work for defense intelligence as it expands to contextualize the breadth of world events. Coordinated attacks on economies and oil and natural gas could mitigate U.S. military strengths and agility.

- **Spread and Miniaturization of Technology:** Globalization is accelerating the pace of technology advancement, which will increasingly penetrate the developing world. While providing new opportunities to many, the interconnection of systems via the Internet also raises the risk of cyber-attack against the national security apparatus. Security and counterintelligence professionals will need to partner with scientific, educational and commercial interests to continuously deny an adversary's ability to acquire and use cyber attack capabilities. The development of new micro-electromechanical machines will offer defense applications, as will the advance of nanotechnology with self-replicating systems, bio-weapons, super-automation capabilities, and artificial intelligence. These developments, while likely to enhance operational support to U.S. war fighters and advance information analysis, may also pose new threats in the hands of adversaries.



- **Changing Workforce Demographics:** Technologically based mobility will change the workforce demographics giving rise to outsourcing and contingent or transient workforces. Managers may be increasingly called upon to supervise a "blended" workforce comprising of traditional employees working alongside contractors, temporary workers or virtual employees. For defense intelligence, this blended workforce will offer increased reach in meeting the extended demand for a culturally diverse and language-enabled workforce, while challenging traditional security and organizational models. In addition, in developed countries including the United States, trends towards an aging population will result in a shortage of workers. For the defense intelligence community, this will require a planned approach to knowledge transfer, ensuring formal and informal data sets are not lost with departing workers.

- **Irregular Warfare Challenge:** The threat of national and transnational insurgencies presents a challenge to many nations and international organizations. In many regions, the irregular challenge shapes the way nations configure their military and security forces, lead their people, and deal with other states in the region. Some irregular movements align themselves with global terror networks, calling upon these groups for guidance, support and legitimacy as they seek to supplant legitimate governments and replace them with dictatorships and theocratic states. Many will seek to align themselves with radicalized states who sponsor irregular warfare and asymmetrical attacks against the United States and like-minded states and interests.

The effects of globalization and the transition towards modernity will reshape the locus of development away from a traditional western viewpoint. They will require us to take significant action to transform the intelligence enterprise in four critical directions: to extend the full advantage of the U.S. intelligence enterprise to all defense users to ensure timely and accurate decisions, as well as ensure defense intelligence is available to the broader U.S. intelligence enterprise under any condition or circumstance; to enhance all services and capabilities provided by the U.S. intelligence enterprise to satisfy changing defense intelligence user needs; to explore concepts, technologies, and strategies to address customer requirements and emerging threats; and, to enable us to counter and deny adversary capabilities to acquire and exploit our technologies or knowledge of the battle space. These actions are required to prepare not only for the strategic shifts we can envision, but—equally important—the "strategic shocks" we cannot.

The Strategy

Defense intelligence is a critical component of the U.S. intelligence enterprise. It has two missions: first, to respond to the unique policy, operational and acquisition requirements of the Department of Defense, and second, to respond to national intelligence missions assigned to the Department of Defense. It comprises the Under Secretary of Defense (Intelligence); national and defense intelligence agencies represented by the NGA, NSA, NRO and DIA; defense organizations such as DSS and CIFA; Service and agency intelligence, counterintelligence and security elements; and joint intelligence components, including those of the Joint Staff and the Combatant Commands. Its customer demands are diverse; from the Commander in Chief and Secretary of Defense to the operational commander and engaged warriors.

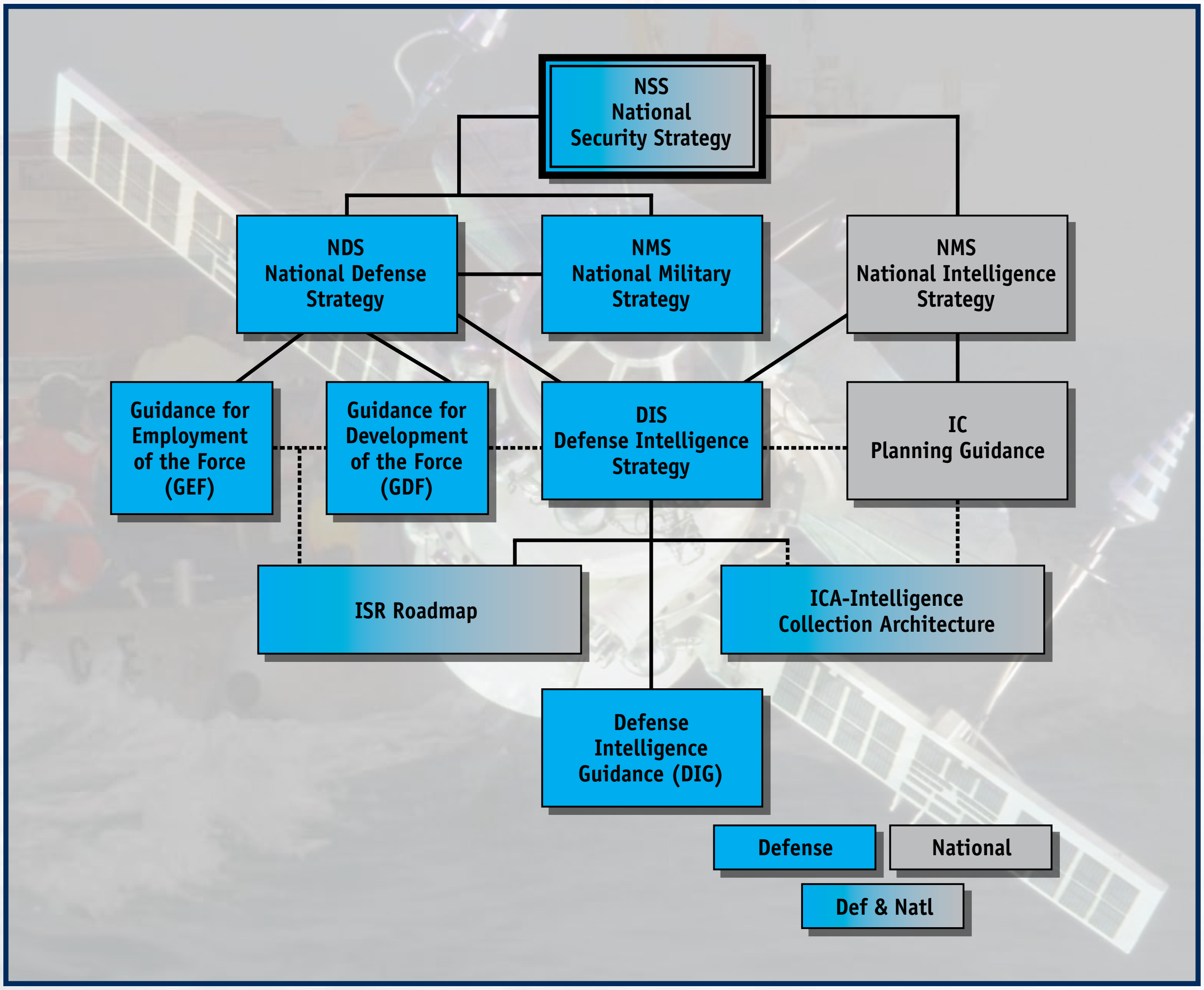


Figure 1. Strategy Hierarchy

As depicted in Figure 1, this first Defense Intelligence Strategy seeks to integrate the two missions by demonstrating how, where and why defense intelligence, counterintelligence, and security activities support the National Intelligence Strategy and respond to requirements of the U.S. military and the Department of Defense. The Defense Intelligence Enterprise must fit seamlessly into a larger network of activities that serves the entire U.S. Government and develops people and systems that also can integrate easily and quickly into the larger network.

This new strategy highlights the following four strategic goals (four **E's**):

❖ **Extend** the full advantage of the U.S. intelligence enterprise to all defense users to ensure timely and accurate decisions, as well as ensure defense intelligence is available to the broader U.S. intelligence enterprise.

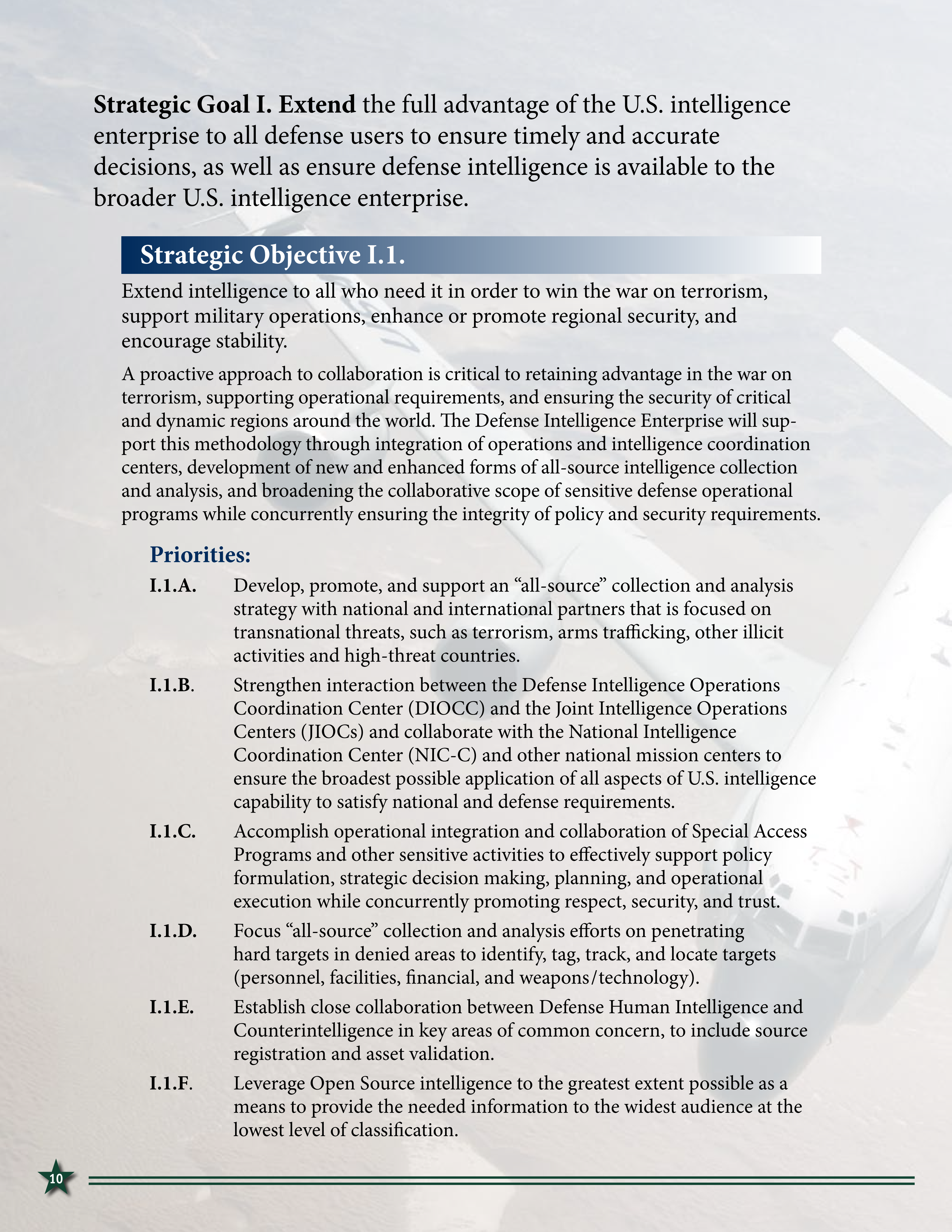
❖ **Enhance** all services and capabilities provided by the U.S. intelligence enterprise to satisfy the changing needs of defense intelligence users.

❖ **Explore** concepts, technologies, and strategies to address customer requirements and emerging threats.

❖ **Enable** us to counter and deny adversary capabilities to acquire and exploit our technologies or knowledge of the battle space.

Ultimately, this strategy will allow all members of the Defense Intelligence Enterprise to see their role in the larger network and every Department of Defense intelligence customer to see how the enterprise will improve its service to them.

Strategic Goals, Strategic Objectives, and Priorities



Strategic Goal I. Extend the full advantage of the U.S. intelligence enterprise to all defense users to ensure timely and accurate decisions, as well as ensure defense intelligence is available to the broader U.S. intelligence enterprise.

Strategic Objective I.1.

Extend intelligence to all who need it in order to win the war on terrorism, support military operations, enhance or promote regional security, and encourage stability.

A proactive approach to collaboration is critical to retaining advantage in the war on terrorism, supporting operational requirements, and ensuring the security of critical and dynamic regions around the world. The Defense Intelligence Enterprise will support this methodology through integration of operations and intelligence coordination centers, development of new and enhanced forms of all-source intelligence collection and analysis, and broadening the collaborative scope of sensitive defense operational programs while concurrently ensuring the integrity of policy and security requirements.

Priorities:

I.1.A. Develop, promote, and support an "all-source" collection and analysis strategy with national and international partners that is focused on transnational threats, such as terrorism, arms trafficking, other illicit activities and high-threat countries.

I.1.B. Strengthen interaction between the Defense Intelligence Operations Coordination Center (DIOCC) and the Joint Intelligence Operations Centers (JIOCs) and collaborate with the National Intelligence Coordination Center (NIC-C) and other national mission centers to ensure the broadest possible application of all aspects of U.S. intelligence capability to satisfy national and defense requirements.

I.1.C. Accomplish operational integration and collaboration of Special Access Programs and other sensitive activities to effectively support policy formulation, strategic decision making, planning, and operational execution while concurrently promoting respect, security, and trust.

I.1.D. Focus "all-source" collection and analysis efforts on penetrating hard targets in denied areas to identify, tag, track, and locate targets (personnel, facilities, financial, and weapons/technology).

I.1.E. Establish close collaboration between Defense Human Intelligence and Counterintelligence in key areas of common concern, to include source registration and asset validation.

I.1.F. Leverage Open Source intelligence to the greatest extent possible as a means to provide the needed information to the widest audience at the lowest level of classification.

Strategic Objective I.2.

Create, promote, and reinforce an information-sharing culture that exemplifies "the responsibility to provide" and "writes for release" while protecting sources and methods in the dissemination of intelligence across the Department of Defense and the Intelligence Community and with international partners.

The Director of National Intelligence has affirmed that the "creation of a culture of collaboration" is a top priority for transformation of the Intelligence Community. This posture recognizes the need to balance access to critical information with the requirement to protect sources and methods. It also creates a culture that embraces and practices operations security and risk management. An interdepartmental and interagency cooperative approach is essential to reduce information voids, confirm sources, and provide enhanced intelligence clarity. This requires a holistic assessment of Defense Intelligence Enterprise information technology requirements in order to achieve the strategic goal of sharing information. Furthermore, this integrated approach is essential to effective policy formulation and successful mission execution. The Defense Intelligence Enterprise will focus efforts to improve and increase cooperation and interoperability with all defense, domestic, national and international homeland defense partners—as well as seek new means to work with international entities. Information developed by operational forces and tactical collectors must be rapidly processed for use at every applicable level, from tactical to strategic, among the Intelligence Community and its partners.

Priorities:

I.2.A. Encourage development of systems, tools, capabilities, training and supporting policies that allow the war fighter and allies at the lowest echelon possible to access all relevant national intelligence data and analysis while simultaneously providing intelligence from fielded forces to higher-level organizations and regional intelligence centers.

I.2.B. Optimize the Defense Intelligence Enterprise's interoperability, cooperation and collaboration by offering access to all intelligence information, tools and processes across multiple agency and operational databases through validated Communities of Interest.

I.2.C. Exchange pertinent defense intelligence with allies and warfighting partners, promote common understanding at every level of the tactical to strategic environment, and build long-term international partnerships that encourage cultural and regional awareness.

I.2.D. Provide users with a tailored common intelligence operational picture (CIOP) and situational awareness concerning the status and availability of intelligence support.

Strategic Objective I.3.

Facilitate Homeland Defense through all-domain (maritime, air, space, land, and cyber) awareness, integration and collaboration with national, homeland defense, law enforcement and international partners.

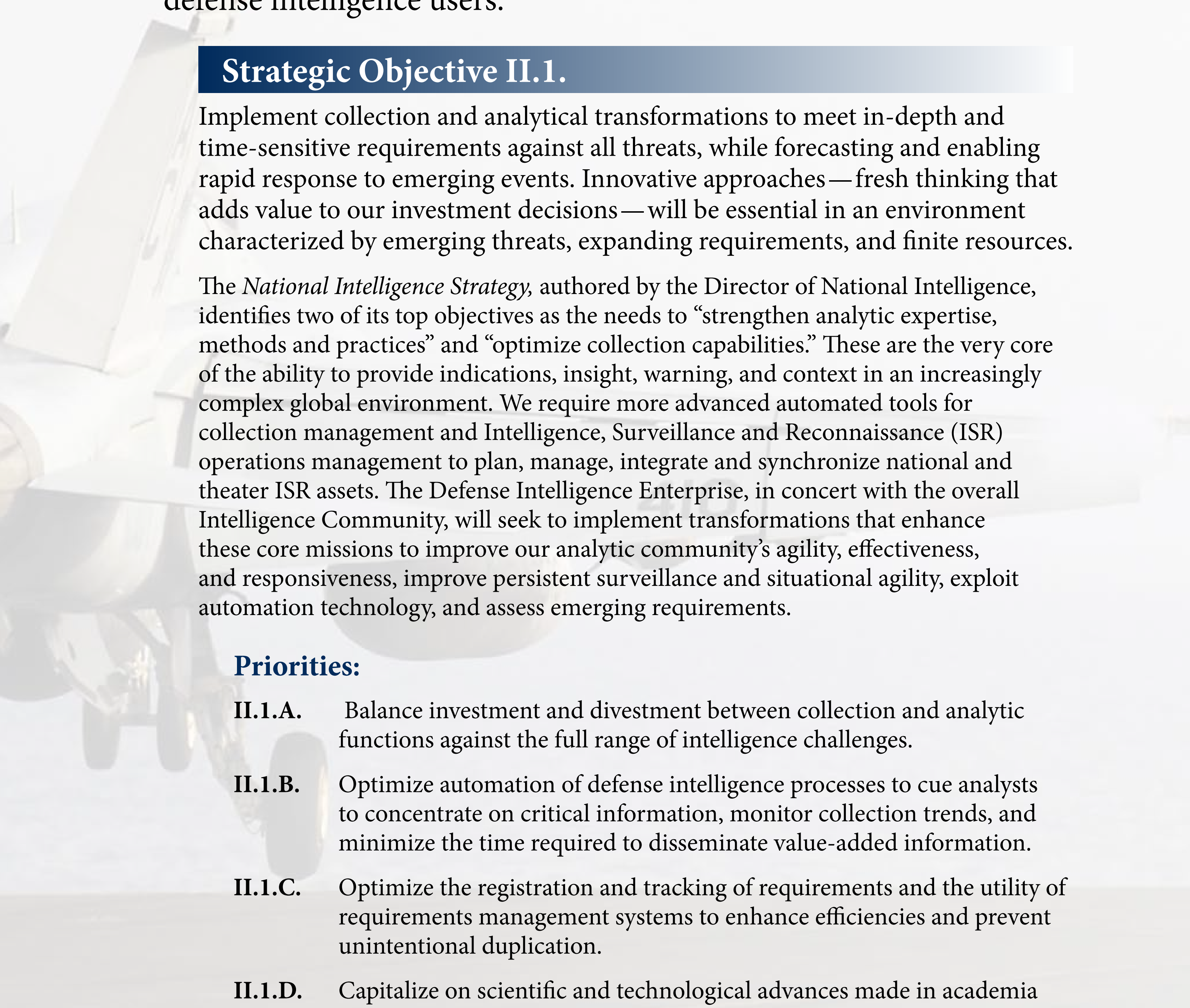
The *National Security Strategy* establishes homeland security as the first priority of the nation and its defenses. New policy and doctrinal concepts must fully leverage defense and national intelligence resources. Innovative tools and methodologies must be created that exploit technological advances and prevent U.S. and allied capabilities from being exploited. These concepts must be incorporated and applied uniformly across organizations and embedded in readiness planning as well as defensive practices.

Priorities:

I.3.A. Promote cooperation with national state, local, tribal and international entities to provide timely intelligence products and services in support of homeland defense.

I.3.B. Encourage and promote robust cyber countermeasures and awareness across the defense infrastructure.

I.3.C. Improve counterintelligence support to computer network operations to facilitate efforts to anticipate, detect, trace, attribute, and counter efforts to exploit and attack U.S. government information systems.



Strategic Goal II. Enhance all services and capabilities provided by the U.S. intelligence enterprise to satisfy the changing needs of defense intelligence users.

Strategic Objective II.1.

Implement collection and analytical transformations to meet in-depth and time-sensitive requirements against all threats, while forecasting and enabling rapid response to emerging events. Innovative approaches—fresh thinking that adds value to our investment decisions—will be essential in an environment characterized by emerging threats, expanding requirements, and finite resources.

The *National Intelligence Strategy,* authored by the Director of National Intelligence, identifies two of its top objectives as the needs to "strengthen analytic expertise, methods and practices" and "optimize collection capabilities." These are the very core of the ability to provide indications, insight, warning, and context in an increasingly complex global environment. We require more advanced automated tools for collection management and Intelligence, Surveillance and Reconnaissance (ISR) operations management to plan, manage, integrate and synchronize national and theater ISR assets. The Defense Intelligence Enterprise, in concert with the overall Intelligence Community, will seek to implement transformations that enhance these core missions to improve our analytic community's agility, effectiveness, and responsiveness, improve persistent surveillance and situational agility, exploit automation technology, and assess emerging requirements.

Priorities:

II.1.A. Balance investment and divestment between collection and analytic functions against the full range of intelligence challenges.

II.1.B. Optimize automation of defense intelligence processes to cue analysts to concentrate on critical information, monitor collection trends, and minimize the time required to disseminate value-added information.

II.1.C. Optimize the registration and tracking of requirements and the utility of requirements management systems to enhance efficiencies and prevent unintentional duplication.

II.1.D. Capitalize on scientific and technological advances made in academia and industry that enable rapid processing, screening, and analysis of large volumes of data, information tagging, archival, and retrieval.

Strategic Objective II.2.

Transform security to streamline processes and protect information.

Personnel recruiting requirements place strenuous demands on the speed and quality of the security clearance process. Current "best practices" must be examined and studied to identify, then introduce, appropriate, relevant methodologies, tactics and techniques to rapidly fill critical and essential intelligence billets without compromising or jeopardizing security. Information and operations security best practices must be identified and developed to protect critical intelligence information and techniques that will deny adversaries the opportunity to exploit information against U.S. and allied operations.

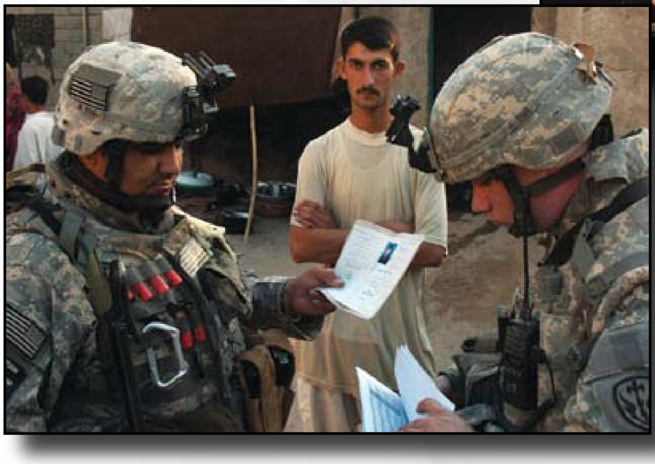
Priorities:

II.2.A. Standardize physical security access control systems and procedures for each level of security in order to ensure interoperability within the Department of Defense and ensure compliance with federal mandates while concurrently recognizing the need for flexibility in developing solutions tailored to meet unique requirements.

II.2.B. Improve the security clearance cycle time by automating the end-to-end processing of investigations.

II.2.C. Adopt common national standards for certification and accreditation of information technology systems processing classified data.

II.2.D. Ensure security classification guidance is up-to-date and users are sufficiently trained to use it so as to protect the Department of Defense mission and national security.



Strategic Goal III. Explore concepts, technologies, and strategies to address customer requirements and emerging threats.

Strategic Objective III.1.

Explore the formation of new, and improve utilization of existing, Defense Intelligence Enterprise professional and sustainment programs to acquire, retain, develop, train, educate, equip, and employ the total workforce effectively and efficiently in support of defense and national intelligence requirements.

There is a direct relationship between the skills of the defense and national intelligence workforce and the quality of intelligence production. Emerging demographic projections and occupational competition will increase competition for employees when building or retaining a quality workforce. Defense intelligence must recognize and understand the motivating factors that draw potential employees to the mission, inspire them to stay and persuade them to leave. Applying human resource tools, incentives, and opportunities is essential if the Intelligence Community is to remain competitive in attracting and retaining persons with critical skills. These efforts should be coupled with the necessary technology in order to enhance the effectiveness of our personnel and expand our services and capabilities.

Priorities:

III.1.A. Transform the Defense Intelligence Enterprise workforce through continuous comparative analysis of workforce capabilities against mission requirements and utilize Defense Civilian Intelligence Personnel System (DCIPS) and industry "best practices."

III.1.B. Establish analytic and collection tradecraft standards and "best practices" and apply them across all levels of the Defense Intelligence Enterprise.

III.1.C. Create a defense intelligence workforce training program that provides the skills and flexibility to leverage all intelligence and security capabilities against the full range of mission requirements.

III.1.D. Maximize the application of technology to identify and reduce redundancy in collection, analysis, and production activities.

III.1.E. Optimize the integration of all components of the total defense intelligence workforce—active and reserve military, federal civilians and contractors—to optimally leverage the unique strengths each offers.

Strategic Goal IV. Enable us to counter and deny adversary capabilities to acquire and exploit our technologies or knowledge of the battle space.

Strategic Objective IV.1.

Overcome the challenges posed by the proliferation of weapons of mass destruction (WMD) across the entire cycle from development through transport and, when unable to prevent their use, the aftermath.

The Joint Chiefs of Staff, writing in the *National Military Strategy to Combat the Weapons of Mass Destruction,* identified intelligence as the primary enabler in the execution of a military strategy intended to "defeat and deter" WMD. The challenge to the Defense Intelligence Enterprise is to understand the capabilities and intentions of state and non-state actors who seek development knowledge, production materials, and delivery systems. The Defense Intelligence Enterprise must combat this threat through focused intelligence that identifies potential threat sources, methodologies, and threat-based protective measures. It must also develop accurate and timely risk assessments for military and civilian planning, decision making and operational use.

Priorities:

IV.1.A. Develop and integrate comprehensive intelligence on illicit research, development, transport, threat, potential targets, and post-use consequences.

IV.1.B. Encourage and promote Defense Intelligence Enterprise situational awareness of regional WMD activities through expanded bilateral and multilateral foreign relationships that are focused specifically on WMD issues.

IV.1.C. Identify and leverage national technical means to assist in implementing the Department of Defense's National Military Strategy to Combat Weapons of Mass Destruction, Consequence Management, and Foreign Consequence Management.

Strategic Objective IV.2.

Develop and employ countermeasures to identify, exploit, and eliminate threats to the Department of Defense and intelligence personnel, technology and assets.

Enhanced global communications offers unrestricted movement of information across international domains and raises the likelihood of threats in and/or from these spheres of influence. Likewise, the exploitation of readily accessible dual-use technology enables our adversaries to develop tools and tactics that can defeat or undermine the strategies of U.S. and allied forces. Intelligence and counterintelligence must respond to current threats and anticipate future events by working with national security and commercial counterparts to stay abreast of and communicate potentially harmful technology developments and increase threat awareness across Department of Defense domains.

Priorities:

IV.2.A. Neutralize illicit "wide nets" cast to collect specific information through an improved cross-flow of information across the counterintelligence community; quickly assess emerging threat trends. Structure counterintelligence to interface seamlessly across defense, industry, other federal departments, and state and municipal entities.

IV.2.B. Anticipate advances in improvised explosive device (IED) technology (triggering devices, warheads, and placement techniques) and anticipate new enemy and adversary tactics, techniques, procedures and technology that could be expected following success in countering IEDs.

Strategic Objective IV.3.

Identify, deny, disrupt and exploit Foreign Intelligence and Security Service (FISS) activities targeting those interests and share information with national-level partners. Support the protection of U.S. and Department of Defense personnel, facilities, technologies, sources and methods.

The Department of Defense Counterintelligence Strategy Fiscal Years 2008–2013 signed by the Under Secretary of Defense for Intelligence on January 2, 2008 charts the course for counterintelligence in the Department. Using the best available methods and technology, the Department of Defense will make every effort to effectively protect its people and interests. As international relationships and cyber activities become more prolific and complex, the sophistication of protection efforts must keep pace and neutralize the threats posed by our adversaries. The Department of Defense will develop and share best practices with its national and international counterparts to ensure all those involved in the intelligence mission are protected.

Priorities:

IV.3.A. Develop counterintelligence training and certification standards and competencies for counterintelligence professionals and foster a cooperative and collaborative environment with HUMINT, Special Operations, Law Enforcement, and national and international partners.

IV.3.B. Identify, deny, disrupt and exploit FISS, international terrorists and their intelligence elements, and insider threats targeting Department of Defense interests.

IV.3.C. In partnership with the ONCIX and FBI, establish security and counterintelligence outreach to the private sector and academia to share information on foreign intelligence threats to emerging U.S. technology.

IV.3.D. The counterintelligence components should develop and sustain integrated and synchronized counterintelligence support to protect Critical Program Information (CPI) with the Department of Defense.

Strategic Objective IV.4.

Eliminate any advantage held by our adversaries to operate from and within the space and cyber domains.

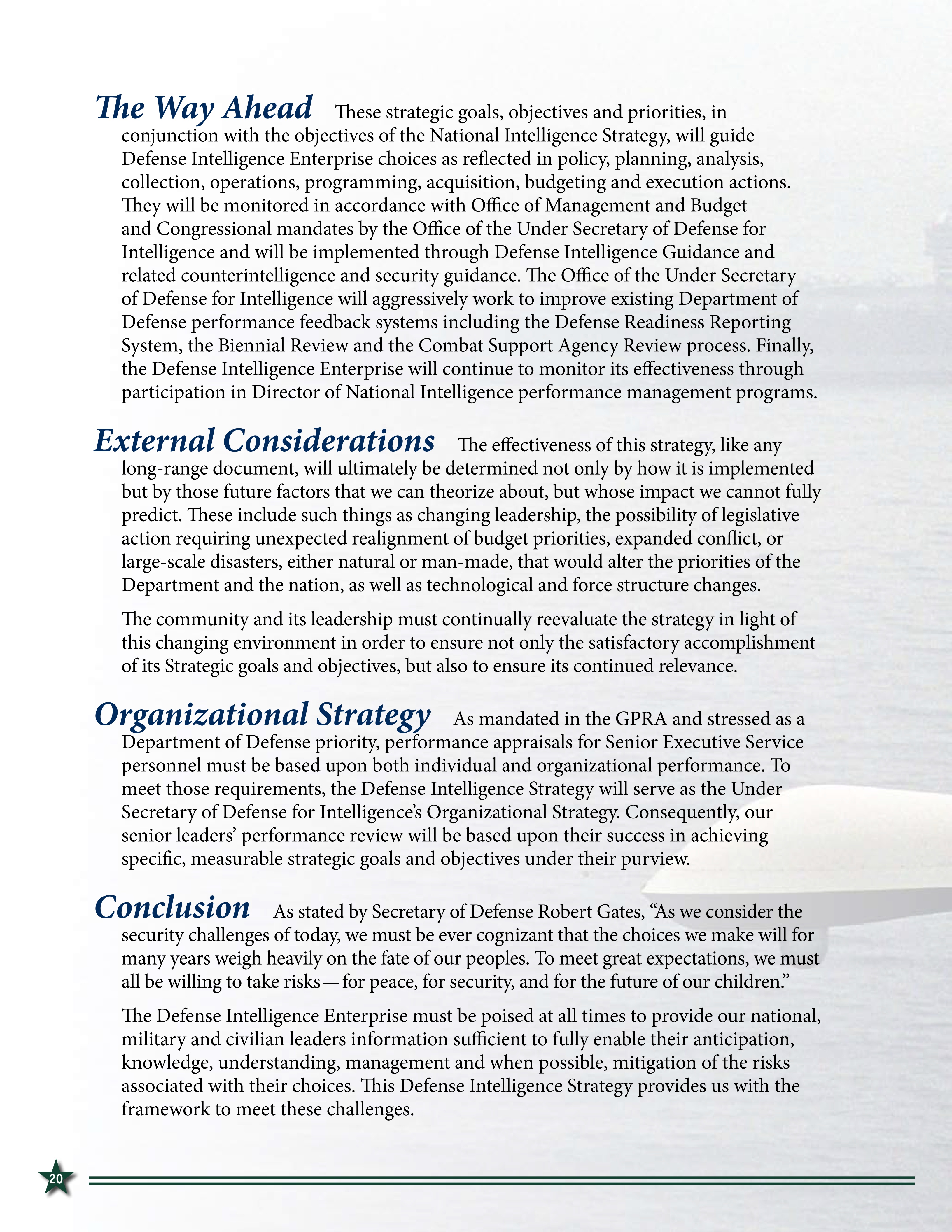
The anticipated increase in global military and commercial space and cyber activities ensures that the focus of defense intelligence professionals employed in these domains will grow exponentially. The potential for the deployment of weapons by near-peer competitors and increasing dependence on space-based assets for military and civilian technologies makes these domains increasingly important. As stated in the *U.S. National Space Policy,* the focus of defense intelligence in space will be to ensure full situational awareness for military and civilian decision-makers, support military planning initiatives, and satisfy operational requirements. As addressed within the Comprehensive National Cybersecurity Initiative, cyberspace has become a vital national interest economically, militarily and culturally, and the current patchwork of passive defense is likely to fail in the face of greater vulnerabilities and more sophisticated threats. Defense intelligence must do its part to defeat this critical threat.

Priorities:

IV.4.A. Pursue and support enhanced space situational awareness to include the protection of U.S. and partners' space assets and interests in all domains.

IV.4.B. Expand our ability to operate from and within the space domain by designing and operating a seamless, fully integrated next generation space enterprise.

IV.4.C. Focus on developing capabilities to attain cyberspace superiority and to protect cyberspace systems with both defensive and offensive countermeasures.



The Way Ahead

These strategic goals, objectives and priorities, in conjunction with the objectives of the National Intelligence Strategy, will guide Defense Intelligence Enterprise choices as reflected in policy, planning, analysis, collection, operations, programming, acquisition, budgeting and execution actions. They will be monitored in accordance with Office of Management and Budget and Congressional mandates by the Office of the Under Secretary of Defense for Intelligence and will be implemented through Defense Intelligence Guidance and related counterintelligence and security guidance. The Office of the Under Secretary of Defense for Intelligence will aggressively work to improve existing Department of Defense performance feedback systems including the Defense Readiness Reporting System, the Biennial Review and the Combat Support Agency Review process. Finally, the Defense Intelligence Enterprise will continue to monitor its effectiveness through participation in Director of National Intelligence performance management programs.

External Considerations

The effectiveness of this strategy, like any long-range document, will ultimately be determined not only by how it is implemented but by those future factors that we can theorize about, but whose impact we cannot fully predict. These include such things as changing leadership, the possibility of legislative action requiring unexpected realignment of budget priorities, expanded conflict, or large-scale disasters, either natural or man-made, that would alter the priorities of the Department and the nation, as well as technological and force structure changes.

The community and its leadership must continually reevaluate the strategy in light of this changing environment in order to ensure not only the satisfactory accomplishment of its Strategic goals and objectives, but also to ensure its continued relevance.

Organizational Strategy

As mandated in the GPRA and stressed as a Department of Defense priority, performance appraisals for Senior Executive Service personnel must be based upon both individual and organizational performance. To meet those requirements, the Defense Intelligence Strategy will serve as the Under Secretary of Defense for Intelligence's Organizational Strategy. Consequently, our senior leaders' performance review will be based upon their success in achieving specific, measurable strategic goals and objectives under their purview.

Conclusion

As stated by Secretary of Defense Robert Gates, "As we consider the security challenges of today, we must be ever cognizant that the choices we make will for many years weigh heavily on the fate of our peoples. To meet great expectations, we must all be willing to take risks—for peace, for security, and for the future of our children."

The Defense Intelligence Enterprise must be poised at all times to provide our national, military and civilian leaders information sufficient to fully enable their anticipation, knowledge, understanding, management and when possible, mitigation of the risks associated with their choices. This Defense Intelligence Strategy provides us with the framework to meet these challenges.

For Information Contact

POLICY, STRATEGY AND DOCTRINE DIRECTORATE

Office of the Under Secretary of Defense for Intelligence

Approved for public release on 31 March 2008 by OSD,
Case #08-S-1190